Everyone's at Risk
Combating the Increasing Threat of Online Fraud and Identity Theft
Questions and Answers from the August 19, 2009
National Phone Forum

These responses are provided within the context of the information presented during this event and are intended to clarify points discussed in the presentation. Due to the public nature of this Q&A, we are able to respond only to general questions relating to the presentation, so some questions were omitted. If you have account questions or client issues, please call the IRS.

Other questions were edited for brevity, clarification or to remove specific identifying references. The responses below should not be considered official guidance independent of the presentation. This information is current as of Nov. 9, 2009. Since changes may have occurred, no guarantees are made concerning the technical accuracy after that date.

1. **Explain compromise of PII (personally identifiable information).**

   Compromise of PII is when an individual's personally identifiable information has been lost, stolen or misplaced.

2. **Is there an IRS link for other governmental agencies which provide tax services to go to if they suspect identity theft such as** Imperial Sugar Company (Public, NASDAQ:IPSU)**?**

   There is not a specific IRS IPSU link resource when identify theft is suspected by other governmental agencies which provide tax services. Internal Revenue Code §6103 places limitations on the types of information the IRS can share with other federal and state agencies, including law enforcement officials, even if it may reveal identity theft. The law includes the general rule that the return and information contained on the return shall be confidential, except as specifically authorized by the statute.

3. **What would prevent someone from using another individual's routing number and account information from a check to pay off a credit card debt via the Internet or telephone?**

   This is not within the scope of work the IRS performs. The responsible parties for addressing this question are credit card companies and financial institutions.

4. **Is it considered full identity theft when an individual has had fraudulent activity on their checking account?**

   Identity theft occurs when someone uses your personallyly identifiable information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. Information on how to determine the signs of identity theft can be found on the FTC's Web site, www.ftc.gov/idtheft/.

5. **Please provide the FTC Web address.**

   The Web URL for the identity theft page on FTC's site is www.ftc.gov/idtheft/.

6. **I received an e-mail from a business that has what appears to be a legitimate Web site, offering to take the name/TIN/address information that my company has gathered for producing our information returns, and to verify it using the IRS matching site for name/TIN information and a USPS database for address information. Is this legitimate?**

   Please forward the email to www.phishing@irs.gov and www.us-cert.gov/.

7. **Can you provide the names of companies to use to secure one's assets?**

   The IRS does not endorse or recommend any private business products, services, or privacy or security policies. We recommend you review information or terms and conditions of companies before making a decision pertaining to your personal affairs.

8. **California Franchise Tax Board has started using account numbers instead Social Security numbers on invoices, filing reminders, and other correspondence sent to taxpayers. When will the IRS begin this practice to deter identity thieves?**

   The IRS is fully dedicated and determined to increase taxpayer safeguards by eliminating or reducing the use of the SSN on taxpayer correspondence as required by OMB Memo 07-16. The IRS submitted a plan to Treasury in February 2009 that outlines its comprehensive approach toward the elimination and reduction of the use of the SSN. However, it is important to understand that legislative constraints preclude the IRS from making any SSN changes on certain tax forms (i.e., Form1040) without change to certain laws.

9. **Is there a policy in development that would require all e-mail hosts to include information to report phishing e-mails posted to each home page?**

   Since the IRS cannot create such a policy, we suggest you address your concerns with the United States Computer Emergency Readiness Team at www.us-cert.gov or the Federal Communications Commission at www.fcc.gov/.

10. **During the last tax season we e-filed a return for one of our audit clients and the return was rejected because someone else claimed an exemption for the taxpayer. According to information provided by the taxpayer, no other taxpayer had the right to claim the exemption. Should the taxpayer have called the hotline under these circumstances?**

    This situation could have been a true case of illegally being claimed as an exemption on someone else's tax return, or a situation where a Social Security number was transferred incorrectly or transposed on the tax return. Visit www.irs.gov to review Publications 4524, Security Awareness and Identity Theft and 4535, Identity Theft Prevention and Victim Assistance. These publications contain valuable information on security awareness, identity theft prevention, victim assistance and how to protect your tax records. After reviewing the publications, your client can then decide whether a call to the Identity Protection Specialized Unit is necessary.

11. **Can a third party report instances of identity theft to the IRS using the IPSU hotline at 800-908-4490?**

    Yes, if an authorized power of attorney is on file with the IRS at the time of the call.

12. **When a report of identity theft is received by IPSU, what is the expected timeframe for investigating an actual instance of tax fraud? What is a consumer to expect?**

    The IPSU does not investigate instances of tax fraud. The IPSU was established to reduce taxpayer burden by providing individualized assistance, including:

    - A single customer service representative to work with each identity theft victim to answer questions and resolve his or her issues.
    - A new and simplified process to verify taxpayer identity and identity theft.
    - A place for taxpayers to self-report identity theft before it affects their tax accounts
    - A place for taxpayers to self-report incidents where they may be at risk for identity theft because their personally identifiable information has been compromised (for example, stolen purse/wallet).

13. **How is a consumer notified of IPSU's findings after an investigation has been completed? Is a notice mailed to the consumer?**

    The IPSU employees will monitor accounts of individuals who are experiencing a tax-related effect of identity theft and when appropriate, they will contact the taxpayer via telephone or through written correspondence.

14. **If a victim of identity theft that has reported the fraud to IPSU receives their tax refund, can they assume that the investigation has been completed in their favor? Does the consumer need to follow-up with IPSU after receiving a refund?**

    The IPSU does not investigate instances of tax fraud. The IPSU was established to reduce taxpayer burden by providing individualized assistance.

15. **If IPSU receives a report of identity theft, does the IRS also notify the state in which the federal return was filed of potential tax fraud? If not, is the consumer notified so that they can contact the state in regards to the fraud?**

    Section 6103 of the Internal Revenue Code places limitations on the types of information the IRS can share with other federal and state agencies, including law enforcement officials, even if it may reveal identity theft. The law includes the general rule that return and return information shall be confidential, except as specifically authorized by the statute.

    A. **Are the tax preparers notified of the fraud?**
       No.

    B. **Are tax preparers investigated by the IRS?**
       Yes, if they are suspected of committing fraud.

16. **Are related agencies (those that may have issued identification, W-2, annual earnings statement, etc.) such as the Department of Motor Vehicles, potential employers, Social Security Administration, etc. notified of potential fraud by the IRS?**

    Section 6103 of the Internal Revenue Code places limitations on the types of information the IRS can share with other federal and state agencies, including law enforcement officials, even if it may reveal identity theft. The law includes the general rule that return and return information shall be confidential, except as specifically authorized by the statute.

17. **The third party designee section on page two of Form 1040 contains a space for a PIN. It is active although I have not used it. What is the security factor in printing a PIN number on the taxpayer's copy especially if someone else has the paper copy?**

    A taxpayer can authorize the IRS to discuss their return with a friend, family member, or any other person they choose. If they check the "Yes" box in the *Third party designee* area of their tax return and provide the information required (designee's name, address and self-selected five-digit PIN), they are authorizing:

    A. The IRS to call the designee to answer any questions that arise during the processing of your return, and
    B. The designee to

a. give information that is missing from to the IRS,
b. call the IRS for information about the processing of the return or the status of your refund or payments,
c. receive copies of notices or transcripts related to the return, upon request, and
d. respond to certain IRS notices about math errors, offsets (see *Refunds*, later), and return preparation.

The authorization will automatically end no later than the due date (without any extensions) for filing the following year's tax return.

In addition to verifying the PIN, the IRS has authentication procedures in place to control discussing any tax account information with a third party designee via telephone. The PIN entry for third party designees is to assist those taxpayers who cannot afford a paid tax preparer to prepare their tax return, or to act on their behalf.

19. Please clarify the Web site for the United States Computer Emergency Readiness Team.

The Web URL for US-CERT is www.us-cert.gov/.

20. Although it is recommended one be cautious when clicking a link contained in an email, is it safe to click on links found on the IRS Web site, specifically Free File, when looking for tax preparers?

By linking to this private business, the IRS is not endorsing its products, services, or privacy or security policies. We recommend you review the business's information collection policy or terms and conditions to fully understand what information is collected by this private business.

Although the IRS tested all approved e-file products, the IRS disclaimer for Free File sites states: ***Please note*** that by clicking on this link, you will leave the IRS Web site and enter a privately owned Web site created, operated and maintained by a private business.

The information that this private business collects and maintains as a result of your visit to its Web site may differ from the information that the IRS collects and maintains. (Please see the IRS Web site privacy and security notice for privacy protections IRS provides to Web site visitors).

21. How quickly does IRS detect persons within its organization who are stealing information from individual tax returns?

The Taxpayer Browsing Protection Act of 1997 forbids the willful unauthorized access or inspection of taxpayer records. Doing so could lead to dismissal of an IRS employee.

22. **Please provide the Web address referred to on slide 16 of the presentation.**

    The Web URL is www.ftccomplaintassistant.gov/.

23. **When forwarding phishing attempts to phishing@irs.gov, confidentiality prohibits the IRS from sharing results of findings from the referral. However, would it be possible for IRS to acknowledge that the referral or forwarded message has been received?**

    This suggestion has been forwarded to the Online Fraud Detection and Prevention office for review and consideration.

24. **How can a taxpayer be assured that a tax preparer does not send the taxpayer's information to be prepared by an outside company?**

    Unfortunately, this is a personal matter between the taxpayer and the tax preparer.

25. **Which agency or IRS department should a preparer contact if it is discovered that a fraudulent federal tax return has been filed with information obtained through ID theft? Who or what department at the IRS could discuss possible sharing of information of a Memorandum of Understanding with a state taxing agency as it relates to identity theft?**

    Section 6103 of the Internal Revenue Code places limitations on the types of information the IRS can share with other federal and state agencies, including law enforcement officials, even if it may reveal identity theft. The law includes the general rule that return and return information shall be confidential, except as specifically authorized by the statute.

25. **Do you have any suggestions for how to speed up processing of a paper return required after the return was rejected using e-file due to Social Security numbers contained on the return?**

    Currently, the IRS cannot speed up this process. If the return is rejected via e-file, mail in the completed Form 1040 and corresponding schedules and forms for processing. The IRS will contact the taxpayer explaining in detail if any additional supporting information is required to process the return. The Taxpayer Advocate Service can be contacted in cases where a taxpayer is experiencing economic hardship.

26. **Has the IRS experienced ID theft from tax returns that have been sent overseas by tax preparers to be processed?**

    The IRS is not aware of any activity such as you have described.